enterprise-2-web

Randy Reitz and Tim Rupp

InterLab 2006

end user overview

- scan-me-now
  - small web based vulnerability scanner
- nessquik
  - powerful web based GUI for Nessus
- splunk
  - log file search engine
- st & e
  - system test, and evaluation checklist

enterprise overview

- inventory
  - near real-time network node inventory
- scanner farm
  - around-the-clock pinger, port scanner and vulnerability scanner
- tissue
  - event issue tracker

scan-me-now

- easy vulnerability scans
- command line or browser
- critical vulnerabilities or all plugins
- can only scan the machine you are coming from
- outputs report to webpage which you can save

http://security.fnal.gov/scanmenow.html

nessquik

- granular control of plugins to use in a scan
- leverage certificates for access control
- scheduled scanning
- monitor your scan progress
- reports in HTML or text
- save scan settings for the future

splunk

- full-text search engine for logs
- combine and search different log sources
- includes an API via SOAP and REST that will likely be used by CST in the future
- very fast, AJAX-ish interface
- able to quickly search massive datasets

http://whoknowswhat.fnal.gov:8000/

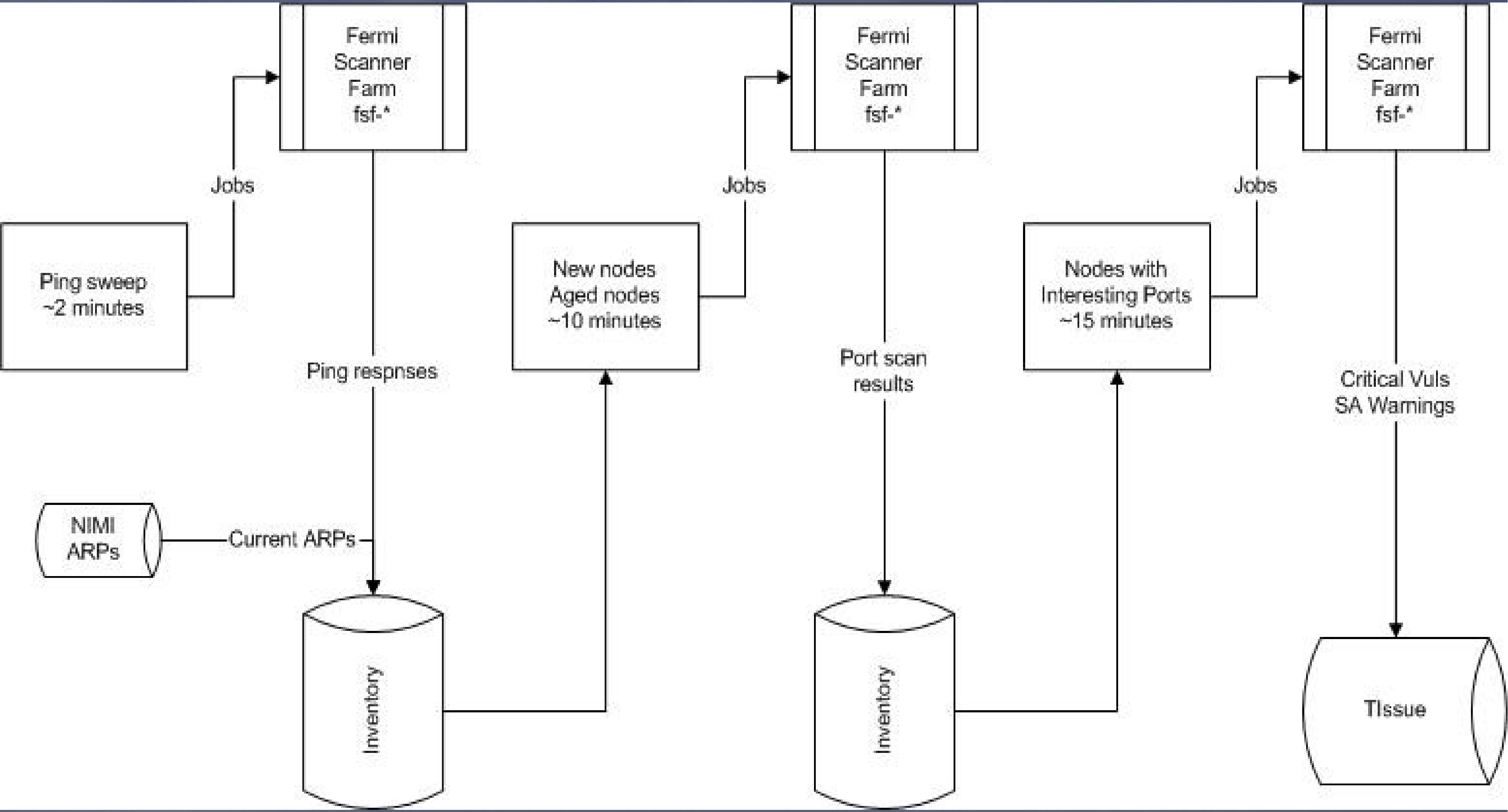
st & e

- traffic lights signal when items have expired, in real-time
- spans + AJAX for fast loading of content
- drop down arrows providing unlimited levels of tasks
- update log, satisfy evaluation
- powerful admin interface to define access
- leverage certificates for access control

inventory

- find active network nodes - ping response or ARP entry
- find aged network nodes
- use nmap port scan to create observation:
  - estimate node OS
  - collect open (listening) TCP ports
- collapse observation in Inventory database
- find recent observations for more scanning

inventory


Fermi
Scanner
Farm
fsf-*
Jobs
Ping sweep
~2 minutes
Ping respnses
NIMI
ARPs
Current ARPs
Inventory
Fermi
Scanner
Farm
fsf-*
Jobs
New nodes
Aged nodes
~10 minutes
Port scan
results
Inventory
Fermi
Scanner
Farm
fsf-*
Jobs
Nodes with
Interesting Ports
~15 minutes
Critical Vuls
SA Warnings
TIssue

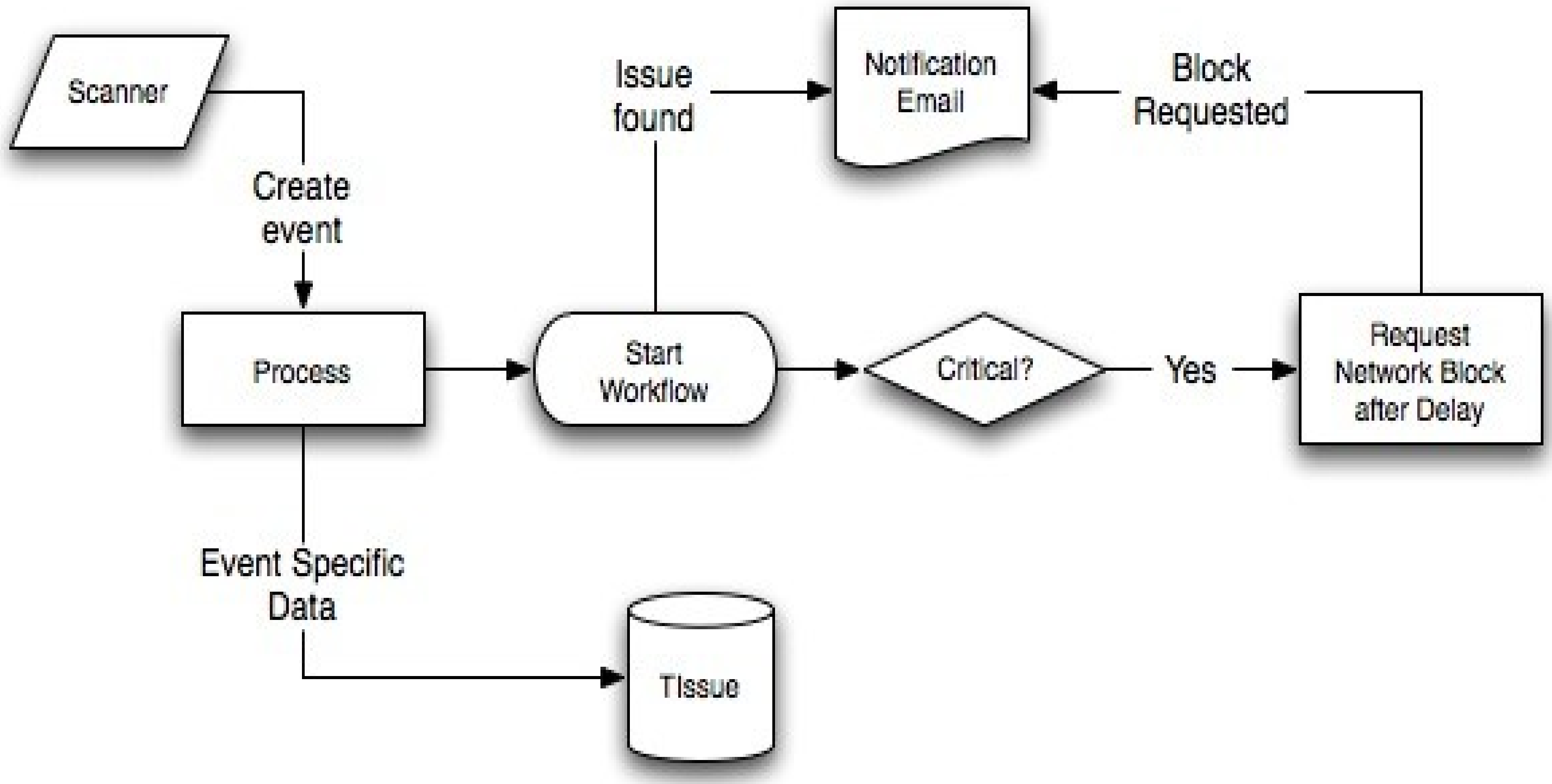
scanner farm

- for nodes with "interesting" services:
  - test node with set of published critical vulnerabilities
  - test node configuration for policy compliance (Kerberos)

TIssue

- create event when scanner finds an "issue"
- find registered info for node
- notify administrator or user
- submit event to work flow

TIssue in brief


Scanner
Create event
Process
Event Specific Data
TIssue
Start Workflow
Issue found
Notification Email
Critical?
Yes
Request Network Block after Delay
Block Requested